AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

United States of America
v.

Fidel Salinas Jr.
USA YOB 1986

Defendant(s)

Case No. M-13-1649-M

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of January 5, 2012 in the county of Hidalgo in the Southern District of Texas , the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. §§ 1030 (a)(5)(B), (b), (c)(4)(A)(i)(I)	Accessing or attempting to access a protected computer without authorization, and as a result of such conduct, recklessly causing damage.

This criminal complaint is based on these facts:

Please see attached Affidavit.

☑ Continued on the attached sheet.

App'd. to file
AUSA

Complainant's signature

Truong T. Nguyen, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: September 11, 2013 3:45 pm

Judge's signature

City and state: McAllen, Texas

Hon. Peter E. Ormsby, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF COMPLAINT

I, Truong T. Nguyen, being duly sworn, hereby depose and state:

1. I am a Special Agent of the Federal Bureau of Investigation (FBI), and have been so employed since April 2010. I am currently assigned to work cyber crime investigations to include computer intrusions, Internet fraud, wire fraud, and health care fraud within the San Antonio, Texas Division.

2. My experience includes the investigation of cases involving the use of computers and the Internet to defraud, to illegally access computers, and to commit financial institution fraud. Since joining the FBI, I have received law enforcement training in the investigation of criminal violations of federal law within the jurisdiction of the FBI, and have received specialized training and gained experience in arrest procedures, search warrant applications, the execution of search and seizures, and various other criminal laws and procedures. I have investigated several cases and participated in the execution of search warrants involving the search and seizure of computer equipment.

3. I make this affidavit in support of the issuance of a complaint and arrest warrant for subject Fidel Salinas, Jr. (SALINAS)

4. The statements contained in this affidavit are based upon my investigation, information provided by other law enforcement officers, and on my own experience and training as a Special Agent of the FBI. Because the affidavit is being submitted for the limited purpose of securing a complaint, I have not included each and every fact known to me concerning the investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that Fidel Salinas Jr. violated 18 U.S.C. § 1030(a)(5)(B).

5. Title 18 U.S.C. §§ 1030(a)(5)(B) and (b) (proscribing attempt)prohibits intentionally accessing or attempting to access a protected computer without authorization, and as a result of such conduct, recklessly causing damage.

6. Title 18 U.S.C. § 1030(e)(2)(B), defines "protected computer" to mean a computer which is used in or affecting interstate or foreign commerce or communication. Additionally, 18 U.S.C. § 1030(e)(8), defines the term "damage" to mean any impairment to the integrity or availability of data, a program, a system, or information.

7. The Hidalgo County (HC) Information Technology (IT) Director (DIRECTOR), advised affiant that on January 5, 2012, an unknown individual, believed to be SALINAS, had attempted to hack (breach) into their website, "www.co.hidalgo.tx.us," specifically their administration management page. HC's website is managed and hosted by CivicPlus on a server located in Kansas City, Kansas. During the early morning, SALINAS made over 14,000 attempts to log into their website server (HC's website and CivicPlus' server). SALINAS' actions affected HC's users, both internal and public. Users would have experienced slowness and latency accessing the main HC website. Additionally, the intrusion attempts were severe enough to prevent the administrators from accessing their website for at least half a day;

subsequently, this prevented employees from managing their own website. The incident required their administrators to contact CivicPlus support specialists in Kansas, for additional support to unlock the user accounts and resecure their systems. Approximately 700 emails were generated by the server as a direct result of SALINAS' hacking activities. The HC website server contained and/or had access links to sensitive data, such as Human Resource data of HC employees and the Emergency Alert System (a component on the website enabling the county to send emergency communication to recipients listed in the database, i.e. during severe weather alerts). DIRECTOR and his IT department spent a tremendous amount of time directly reacting to the effects of the intrusion. DIRECTOR quantified a total of approximately $10,620.32, in damages and loss incurred by the county in response to the incident.

8. An HC employee in Operations Administration and Public Affairs advised affiant that the information, access links, and data on the HC website from January 5, 2012 have remained virtually the same as ~~it does today~~ of, June 12, 2013. Specifically, with regards to the administration of justice for the people of HC, the ability to pay court fines through the web site, bail bondsman's access to court related matters, and HC court case records were the same as currently available through the web site.

9. A CivicPlus Support Specialist (SPECIALIST) provided Hidalgo County Sheriff's Office (HCSO) and FBI a log of the approximately 14,000 intrusion attempts that occurred on January 5, 2012. Specifically, the log recorded the Internet Protocol (IP) address, which identified the originating location of the hacker, and the random assumed user account names used during the intrusion attempts to hack into the HC website server. According to SPECIALIST, the hacker used brute force (brute force is an exhaustive method of systematically checking all possible keys until the correct key is found) to attempt to breach the administration login page. SPECIALIST stated that Salinas was not authorized to access their administration webpage.

10. Further investigation revealed that the IP address from where the hacking attempt originated was an address on Nolana Loop in Donna, Texas. On January 11, 2012, HC executed a state search warrant at said location. The investigators discovered that the property owner's wife was the registered account holder. The property owner said that SALINAS was his daughter's boyfriend who had moved into the home. An HCSO investigator interviewed SALINAS who admitted that he attempted to gain access to the HC website after he saw a flaw. SALINAS acknowledged that everything he did to the county's computer system was wrong. Investigators recovered multiple laptop computers, computer towers, external storage devices and other electronic devices from the residence.

11. FBI Computer Analysis Response Team (CART), pursuant to a federal search warrant, returned a complete analysis report on the computer devices seized from SALINAS. FBI CART found the following derogatory information on SALINAS' computer:

- A website vulnerability tool, Acunetix Web Vulnerability Scanner, had been downloaded and installed on SALINAS' computer. A report produced by the application was found logging the intrusion attempts against the HC website. A file titled "www.co.hidalgo.tx.us Scan Report" was created January 5, 2012 at 1:48am and found on SALINAS' Windows desktop as a shortcut file.

- A Havij tool was installed on SALINAS' computer. A Havij tool is an automated SQL injection tool that helps penetration testers find and exploit SQL Injection vulnerabilities on a web page.

- Google search and website visits were found on the SALINAS' computer system relating to the "Anonymous" hacker group.

- An Internet Relay Chat (IRC) file, which contained approximately six months of chat logs for the hacking group Anonymous' Operation Anti-Security (Operation AntiSec) faction, was found.

12. On September 19, 2012, FBI Special Agent Christopher Wallingsford interviewed SALINAS. SALINAS stated he used a program on his computer in an attempt to gain administrative access to the website. SALINAS claimed that he was not trying to do anything illegal but thought that if he gained access SALINAS would pass on that information to the Hidalgo County Network Administrator as a courtesy. SALINAS did not remember the name of the program that he used to gain access, but did say it was a SQL injection software tool.

13. On May 14, 2013, SALINAS was interviewed by Affiant. Salinas admitted to executing the Havij application (an advanced SQL injection tool), Acunetix Web Vulnerability scanner, and his own custom written script to access the HC website server. He admitted that he was "stupid" for using the brute force technique. He admitted to chatting with Anonymous users via chat. He also said if he had found something derogatory on Sheriff Lupe Trevino on the system, he would have given the information to authorities or publicized it himself. SALINAS confirmed he made statements directed at the Sheriff on January 22, 2012, on his Facebook.com page:

   - "F**K [redaction added] you corrupt officials and politicians, When someone tries to give you advice that your servers aren't secure and said person doesn't modify, access or download and "redistricted" information. I believe you say thank you instead of being afraid of what you don't know by getting an invalid warrant, arresting and wrongfully jacking all his electronics. – We do not forgive, we do not forget, divide by zero we fall, EXPECT US!" (SALINAS' end quote is used by Anonymous and "hacktivist" groups).

14. SALINAS further stated that he believed the HC web server contained voter registration, social security numbers, personal identification of people, and employee human resource and payroll information. When affiant asked what SALINAS believed the HC website server experienced as a side effect of his intrusion attempts, he responded with the following:

- Users would not have access to the website or access the database on the server.
- Bandwidth would have been affected, resulting in slowness to the public users accessing the HC website.
- Administrators would have gotten emails as a result of his intrusion attempts. Because he used the brute force technique, user accounts were caused to be disabled. Subsequently, he estimated approximately 5,000 emails would have been generated as a result and could slow down the email server.